

Quantum benchmarking with realistic states of light

N. Killoran¹, M. Hosseini², B. C. Buchler², P. K. Lam², and N. Lütkenhaus¹

¹ *Institute for Quantum Computing and Department of Physics & Astronomy,
University of Waterloo, N2L 3G1 Waterloo, Canada and*

² *Centre for Quantum Computation and Communication Technology, Department of Quantum Science,
The Australian National University, Canberra, ACT 0200, Australia.*

(Dated: March 3, 2013)

The goal of quantum benchmarking is to certify that imperfect quantum communication devices (e.g., quantum channels, quantum memories, quantum key distribution systems) can still be used for meaningful quantum communication. However, the test states used in quantum benchmarking experiments may be imperfect as well. Many quantum benchmarks are only valid for states which match some ideal form, such as pure states or Gaussian states. We outline how to perform quantum benchmarking using arbitrary states of light. We demonstrate these results using real data taken from a continuous-variable quantum memory.

I. INTRODUCTION

Quantum communication is poised to be the first real-world application of quantum information theory. Impressive efforts are underway to build advanced quantum devices, such as quantum channels [1], quantum memories [2], and quantum key distribution systems [3], which will make long-distance quantum communication a reality. But our control over the quantum world is still imperfect; it is difficult to create devices whose operation faithfully matches the ideal. Internal flaws and external influences can negatively impact a device's operation. Since quantum effects are very fragile, there is little tolerance for such deficiencies. Fortunately, it is still possible for imperfect devices to facilitate quantum communication.

The task of *quantum benchmarking* is to certify a device to be within the “quantum domain,” the operational regime where an imperfect device is still useful for quantum communication. In practice, this is done by preparing some test states, probing the device in question with these states, and making measurements on the resulting output states. The corresponding theoretical task is to calculate the threshold (according to some figure(s) of merit) between a quantum device and the best comparable classical device. If we can conclude, based on the available information, that the device's performance beats the benchmark value, then the device is in the quantum domain. Of course, there is some interplay between the two sides, especially in the choice of test states.

A number of benchmarks have been developed in recent years, especially for continuous variable (CV) encodings of light [4–21]. Many of these benchmarks require test states which are pure and/or Gaussian. Such states are much more amenable to theoretical analysis than more general states of light. Now, if we recognize that our quantum communication devices are imperfect, we must also recognize that our state preparations may be imperfect as well (e.g., due to excess noise or other flaws in the preparation procedure). This leads to dis-

crepancies between the idealized benchmarking situation and the experimental realization. Using state tomography or some other process to obtain numerical descriptions of the prepared states, we may find that these states are not consistent with the ideal form (e.g., not pure or not Gaussian). In this case, is it valid to apply benchmarks which assume the ideal form? Furthermore, many of the above benchmarks require an infinite ensemble of test states. What conclusions can be made when using a finite ensemble (as we must always do in practice) if the benchmark requires an infinite ensemble? Addressing these practical concerns is an important part of quantum benchmarking.

In this work, we present a general benchmarking framework which is easily adaptable to different testing conditions. In particular, our framework allows for quantum benchmarking using arbitrary states, not just states with a special form. Previous progress has been made toward this goal using *entanglement-based* benchmarks, but these schemes are still limited to special cases: either the test ensemble contains only pure states [15–17, 19], or it consists of only two mixed states [18] (in either case, the states are not required to be Gaussian). We extend these results to any finite number of mixed states, allowing us to derive quantum benchmarks for arbitrary finite ensembles of test states. There is some freedom allowed by this extension, and we outline how to strengthen benchmarks to give the largest quantum domain, i.e., the best chance of certifying imperfect quantum devices. We then apply our benchmarking criterion to an actual continuous-variable memory.

The remainder of this paper is laid out as follows. In Sec. II we outline the necessary theory. We show how to generalize previous results to an arbitrary number of test states and how to optimize this generalization. As an application, we consider phase-symmetric test ensembles, and derive a simple standard form for the bipartite matrices used to represent such ensembles in entanglement-based benchmarking. In Sec. III, we test our general benchmarking method using data from a real continuous-

variable memory. Finally, in Sec. IV, we make some concluding observations.

II. ENTANGLEMENT-BASED QUANTUM BENCHMARKING

A. Benchmarking background

We picture any potential quantum communication device as a channel which takes quantum states as input and gives quantum states as output. The distinction between quantum and classical communication devices is that classical devices are equivalent to *measure and prepare* (MP) channels. In these channels, the input state is measured, the measurement outcome is communicated or stored in a solely classical manner, and an output state is prepared based on this classical data. Any device that is equivalent to a MP channel is not a true quantum communication device, since communication through MP channels is equivalent to classical communication. It is often convenient to picture benchmarking in an adversarial way. In this scenario, we allow the possibility that a quantum device could have been replaced by a MP channel trying to pass our quantum benchmarking tests. Only by conclusively ruling out MP operation can we certify a quantum device as genuine. Devices which can be discriminated from classical channels are said to be in the quantum domain.

In practice, we probe the device with a finite number of different test states $\{\rho_k\}_{k=0}^{M-1}$ and make measurements on the resulting output states. From the measurement results and knowledge of the test ensemble, we must determine whether the device is in the quantum domain or whether the same operation could be performed by a classical channel. With enough test states and measurements, we can characterize a device exactly, i.e., perform process tomography, allowing a device's performance to be tested against any theoretical benchmark [22, 23]. However, process tomography can be resource intensive, especially for CV systems. Our goal will be to certify quantum devices with minimal requirements. If a given benchmarking test fails, it may still be possible to certify a quantum device by incorporating more test states and/or more measurements.

There are a number of approaches for determining whether a device is in the quantum domain. Typically, some specific operational or theoretical quantities are chosen and the corresponding quantum domain is mapped out by determining the limits of classical devices. One such example is the state-independent T - V benchmark based on signal-transfer and conditional-variance [12, 24], parameters which capture how well a signal is preserved and how much extra noise is introduced by the device. Another much-studied figure of merit is the average fidelity between the test states and the corresponding output states after the device action (represented by the

map Λ):

$$\bar{F} = \sum_{k=0}^{M-1} p_k F(\rho_k, \Lambda[\rho_k]), \quad (1)$$

where p_k are some fixed weights. If the test states are not perfectly distinguishable, a MP channel cannot achieve perfect fidelity. Indeed, for a given test ensemble, there is some maximum average fidelity \bar{F}_{MP}^{\max} which is achievable by MP channels. A device must beat this benchmark value, $\bar{F} > \bar{F}_{MP}^{\max}$, to be in the quantum domain. This approach requires us to compute the optimal value \bar{F}_{MP}^{\max} and to calculate or bound the experimentally-achieved value \bar{F} . Typically, finding the experimental fidelity requires tomography on the output states. As well, tomography on the prepared states is needed to ensure that they match the required form.

A number of fidelity-based benchmarks have been derived for CV test states, including coherent states, squeezed states, and thermalized states [4, 5, 7–11, 13]. Other benchmarks use the same approach but slightly different figures of merit [11, 14] or models for classical channels [6]. Many of these benchmarks require test ensembles with an infinite number of states, although fidelity benchmarks for any two pure states have also been calculated [8, 26]. The classical threshold \bar{F}_{MP}^{\max} is often very difficult to determine, making the fidelity-based approach hard to generalize to arbitrary test ensembles. This limits the applicability of this method to those ensembles where a benchmark value has been found, and we must verify that the experimentally-prepared states match the ideal form. As well, without (costly) tomography on the output states, or extra assumptions, it can be difficult to properly determine the experimental fidelity value \bar{F} .

There is another approach to quantum benchmarking [15–21] which avoids many of these problems. This approach is based on the following important property: MP channels always break entanglement. In fact, the set of MP channels is equivalent to the set of entanglement-breaking channels [27]. By showing that a device preserves entanglement, we can exclude it from the MP class. To accomplish this goal, a bipartite entangled state, built from the test states, is considered. For the moment, we will focus on pure test states $\rho_k = |\psi_k\rangle\langle\psi_k|$, and we will generalize to mixed states in the next subsection. We imagine the test states are coupled with an ancillary system, giving the following entangled state

$$|\Psi^{\text{ent}}\rangle_{AA'} = \frac{1}{\sqrt{M}} \sum_{k=0}^{M-1} |k\rangle_A |\psi_k\rangle_{A'}. \quad (2)$$

Here, Alice's states lie in an M -dimensional Hilbert space for which $\{|k\rangle_A\}_{k=0}^{M-1}$ forms an orthonormal basis. We let the device in question act on the A' subsystem of this entangled state, mapping it to some output system B , while subsystem A is kept isolated. The reduced state

ρ_A remains the same, independent of the channel:

$$\langle k | \rho_A | l \rangle = \frac{1}{M} \langle \psi_l | \psi_k \rangle. \quad (3)$$

Aside from a fixed prefactor, the density matrix ρ_A is the Gram matrix (matrix of overlaps) for the pure test states $\{|\psi_k\rangle\}$. This structure will be important when we generalize to arbitrary states in the next subsection.

Performing the local projective measurements $\{\hat{\Pi}_A^k := |k\rangle\langle k|_A\}_{k=0}^{M-1}$ on $|\Psi^{\text{ent}}\rangle_{AA'}$ effectively prepares the test states $\{|\psi_k\rangle_{A'}\}_{k=0}^{M-1}$ at random. After passing through the channel, the output states $\{\rho_k^{\text{out}} := \Lambda(|\psi_k\rangle\langle\psi_k|)\}_{k=0}^{M-1}$ (on the system B), are measured with some fixed set of measurements $\{\hat{O}_B^j\}$. Using only these measurement results and knowledge of the Gram matrix ρ_A , we aim to determine whether the state $\rho_{AB}^{\text{out}} = [\text{id}_A \otimes \Lambda]|\Psi^{\text{ent}}\rangle\langle\Psi^{\text{ent}}|_{AA'}$ is entangled.

One method to certify entanglement is with a witnessing procedure [15–17, 19]. On the other hand, it can be useful not only to qualify entanglement, but also to quantify it. An alternative approach to entanglement-based benchmarking [20, 21] is therefore to bound the entanglement of the final state away from zero using some suitable entanglement measure \mathcal{E} , i.e., to show $\mathcal{E}(\rho_{AB}^{\text{out}}) > 0$. One advantage of the quantitative method is that it can be used to compare different devices or situations which fall in the quantum domain. When we demonstrate our benchmarking method in Sec. III, we will take the quantitative approach, using tools from [21].

The measurements on system A are restricted to the projections $\{\Pi_A^k\}_{k=0}^{M-1}$. Performing more general measurements on system A would prepare superpositions of the test states. But these superposition states can simply be included in the test ensemble, offering the same formalism with a slightly different entangled state for Eq. (2). This source replacement scheme allows us to work with the test states in practice and consider the entangled state $|\Psi\rangle_{AA'}$ as a virtual construct. The Gram matrix ρ_A provides the theoretical link between the test states and the virtual entangled state.

Finally, the Gram matrix compactly contains all information about the pure test states which is needed for the given benchmarking procedure. A full description of the test ensemble is not strictly necessary. Of course, we require some method for determining the overlap information. State tomography is one way to obtain this, but there may be other less costly ways to constrain the Gram matrix. Similarly, we do not require tomography on the output states for entanglement-based benchmarking. Indeed, previous papers have demonstrated that useful quantum benchmarks can be found by measuring only two conjugate quadratures [1, 15–21, 28]. Thus, entanglement-based benchmarking can be very practical from an experimental point of view.

B. Entanglement-based picture for arbitrary states

How can the entangled state in Eq. (2) be extended to the case where the test states $\{\rho_k\}_{k=0}^{M-1}$ are mixed? Some progress was made in this direction in [18], restricting to the case of only two test states. Among several potential ways to generalize Eq. (2), it was found that using purifications of the test states was the most useful. In this framework, we imagine that instead of preparing the test states, we prepare purifications $\{|\Gamma_k\rangle_{A'A''}\}_{k=0}^{M-1}$, where A'' is some purifying system, i.e.,

$$\text{Tr}_{A''}(|\Gamma_k\rangle\langle\Gamma_k|_{A'A''}) = \rho_k. \quad (4)$$

From now on, $|\Gamma_k\rangle$ will always refer to a purification of ρ_k .

To clarify, the experimental procedure (using the test states $\{\rho_k\}$) remains the same. Theoretically, the benchmarking procedure is analyzed as if the purifications $\{|\Gamma_k\rangle_{A'A''}\}$ were used instead, i.e., the device is allowed to act on the larger system $A'A''$. Measurements are still restricted to the B subsystem, and the only information we retain about the purifications for the final benchmarking are the overlaps $\langle\Gamma_k|\Gamma_l\rangle$. In this way, we give extra power to an adversarial MP device, since the purifications may be more easily distinguished than the test states. Although this modification may result in a slightly smaller quantum domain, any benchmarks based on the purifications are valid. Now, even though we give extra power to an adversarial device, we should still aim to make our quantum benchmarks as stringent as we can, i.e., to keep the quantum domain as large as possible. Ref. [18] offers one method to limit the adversarial advantage provided by purifications, but this introduces additional numerical complexity, and we will not consider it in the present paper. However, there still remains some freedom in the actual choice of purifications, which we can use to strengthen our benchmarking scheme.

For two mixed test states ρ_0 and ρ_1 , the virtual entangled state takes the form

$$|\Psi\rangle_{AA'A''} = \frac{1}{\sqrt{2}} \left(|0\rangle_A |\Gamma_0\rangle_{A'A''} + |1\rangle_A |\Gamma_1\rangle_{A'A''} \right). \quad (5)$$

Purifications are not unique, but we must fix some choice to proceed further. Since we only retain information about the overlap $\langle\Gamma_0|\Gamma_1\rangle$, it is important to know the range of allowed values for this parameter. We can always find purifications which are orthogonal. On the other hand, from Uhlmann's theorem [29, 30], we have

$$\max_{|\Gamma_0\rangle, |\Gamma_1\rangle} |\langle\Gamma_0|\Gamma_1\rangle|^2 = \left[\text{Tr} \sqrt{\sqrt{\rho_0} \rho_1 \sqrt{\rho_0}} \right]^2 =: F(\rho_0, \rho_1), \quad (6)$$

where $F(\rho_0, \rho_1)$ is the fidelity between the two test states. Thus, the range of allowed overlaps is $|\langle\Gamma_0|\Gamma_1\rangle|^2 \in [0, F(\rho_0, \rho_1)]$. In [18], it was argued that the best benchmarks (i.e., those which give the best opportunity to

certify devices in the quantum domain) come from purifications which saturate the Uhlmann fidelity bound. There was numerical support for this claim, but one can also appeal to the fact that the fidelity is a measure of (in)distinguishability. Accordingly, choosing purifications which are as indistinguishable as possible will make it harder for a MP channel to simulate a quantum channel reliably. We will make this intuition more precise in the following pages. Finally, we note that Uhlmann's theorem has also been suggested for fidelity-based benchmarking using two mixed states [8].

It is straightforward to generalize the entangled state in Eq. (5) to accomodate $M > 2$ mixed states. Specifically, we will use

$$|\Psi\rangle_{AA'A''} = \frac{1}{\sqrt{M}} \sum_{k=0}^{M-1} |k\rangle_A |\Gamma_k\rangle_{A'A''}. \quad (7)$$

The reduced density matrix $\rho_A = \text{Tr}_{A'A''} |\Psi\rangle\langle\Psi|_{AA'A''}$ is now (aside from the prefactor) the Gram matrix of the purifications $\{|\Gamma_k\rangle\}_{k=0}^{M-1}$:

$$\langle k | \rho_A | l \rangle = \frac{1}{M} \langle \Gamma_l | \Gamma_k \rangle. \quad (8)$$

It is *not* straightforward how to choose purifications in this case. The fidelity is a useful measure for two states, but there is no clear extension of the concept for multiple states. Indeed, the set of allowed values for the overlaps $\langle \Gamma_k | \Gamma_l \rangle$ has a more subtle structure than just a product of the ranges allowed by Eq. (6). It may not be possible to choose purifications which achieve the fidelity bound for all pairs. In order to determine the best choice of purifications, we will examine the structure of entanglement-based benchmarking at a deeper level.

C. Optimizing the purifications

How can we choose purifications to optimize the strength of entanglement-based benchmarks based on multiple mixed test states? To begin answering this, we make the following observation.

Proposition 1. Let $\{|\Gamma_k\rangle\}_{k=0}^{M-1}$ and $\{|\Delta_k\rangle\}_{k=0}^{M-1}$ be two different sets of purifications of the test states $\{\rho_k\}_{k=0}^{M-1}$. Assume that there is a completely positive, trace-preserving (CPTP) map which transforms one set of purifications to the other, i.e., there exists Ω such that

$$\Omega[|\Gamma_k\rangle\langle\Gamma_k|] = |\Delta_k\rangle\langle\Delta_k| \quad (9)$$

for all k . If we cannot conclude that a device is in the quantum domain with information based on the $\{|\Delta_k\rangle\}$, then we cannot conclude that the same device is in the quantum domain using information about the $\{|\Gamma_k\rangle\}$.

Proof. Represent the device under investigation by the map Λ . This map takes in states on the joint $A'A''$ system and outputs states on the B system. We proceed in

two steps. First, we assume that we can perform tomographically complete measurements on the output states. Later we will relax this to incomplete measurements. In either case, we work under the constraint that, for all k ,

$$\Lambda[|\Delta_k\rangle\langle\Delta_k|] = \Lambda[|\Gamma_k\rangle\langle\Gamma_k|] = \rho_k^{\text{out}}, \quad (10)$$

where ρ_k^{out} is the output state corresponding to the test state ρ_k . This constraint is experimentally enforced, since the output states are independent of the purification we use to theoretically describe the protocol. Consider the case where we describe the test states using the purifications $\{|\Delta_k\rangle\}$. A benchmarking protocol is unsuccessful when we cannot discriminate between the device and a MP channel, i.e., when there is a MP channel which gives the same output states as the device. Assume then that there exists an MP channel $\tilde{\Lambda}_{MP}$ such that

$$\tilde{\Lambda}_{MP}[|\Delta_k\rangle\langle\Delta_k|] = \rho_k^{\text{out}} \quad (11)$$

for all k . Now consider the alternate situation where we use the purifications $\{|\Gamma_k\rangle\}$, and there exists a CPTP map Ω as in Eq. (9). We define another channel Σ_{MP} by

$$\Sigma_{MP} := \tilde{\Lambda}_{MP} \circ \Omega. \quad (12)$$

The concatenation of any channel with a MP channel is as a MP channel, so Σ_{MP} is in the MP class. From Eqs. (9-11), we must have

$$\Sigma_{MP}[|\Gamma_k\rangle\langle\Gamma_k|] = \rho_k^{\text{out}} \quad (13)$$

for all k . Therefore, there exists a MP channel which gives the observed output states when using the purifications $\{|\Gamma_k\rangle\}$.

Even when we do not have enough measurements for complete tomography, we can follow similar arguments. Instead of having one output state ρ_k^{out} for every k , we have a set of states $\mathcal{C}[\rho_k^{\text{out}}]$, all of which have the same expectation values with respect to the employed measurement operators $\{\hat{O}_B^j\}$:

$$\mathcal{C}[\rho_k^{\text{out}}] := \{\tau | \text{Tr}(\tau \hat{O}_B^j) = \langle \hat{O}_B^j \rangle_{\text{meas}} \forall j\}. \quad (14)$$

In this case, a benchmarking protocol is unsuccessful when there is a MP channel Λ_{MP} such that

$$\tilde{\Lambda}_{MP}[|\Delta_k\rangle\langle\Delta_k|] \in \mathcal{C}[\rho_k^{\text{out}}] \quad (15)$$

for all k . Using this channel, we again define a MP channel Σ_{MP} as in Eq. (12). By Eqs. (9) and (15), we conclude

$$\Sigma_{MP}[|\Gamma_k\rangle\langle\Gamma_k|] \in \mathcal{C}[\rho_k^{\text{out}}]. \quad (16)$$

In either case, if benchmarking is unsuccessful for the $\{|\Delta_k\rangle\}$, it cannot be successful for the $\{|\Gamma_k\rangle\}$. \square

This proposition has some important consequences. For one, it tells us that in the source-replacement scheme we are using, the quantity of entanglement does not have

a direct significance [31]. Instead, the focus should be to find those purifications which cannot be collectively transformed, via CPTP maps, to any other valid set. Benchmarking schemes built with such purifications provide the hardest challenge for an adversarial MP device attempting to mimic a true quantum device. Indeed, such limiting purifications necessarily lead to a larger quantum domain than any other comparable choice. Because we only use the overlaps for benchmarking, we can optimize the CPTP map condition on the level of Gram matrices. In the rest of this paper, we will use the terms ‘purifications’ and ‘Gram matrix (of the purifications)’ somewhat interchangeably.

The following theorem will help us translate the CPTP map condition to a more amenable form.

Theorem 1 ([32–34]) *Let $\{|\gamma_k\rangle\}_{k=0}^{M-1}$ and $\{|\delta_k\rangle\}_{k=0}^{M-1}$ be two sets of pure states (they do not need to be purifications). Let G and D be the corresponding Gram matrices, with elements $G_{ij} := \langle\gamma_j|\gamma_i\rangle$ and $D_{ij} := \langle\delta_j|\delta_i\rangle$. There exists a CPTP map Ω taking the former states to the latter if and only if the Gram matrices are related by*

$$G = P \circ D, \quad (17)$$

where \circ denotes the Hadamard (or Schur or entrywise) product. The matrix P satisfies $P \geq 0$ and its diagonal elements are given by $\text{diag}(P) = \{1, 1, 1, \dots\}$.

To avoid potential confusion, we point out that while the CPTP map Ω takes the $\{|\gamma_k\rangle\}$ to the $\{|\delta_k\rangle\}$, the Gram matrix condition, Eq. (17), has the opposite sense, i.e., G is obtained by doing a particular operation on D . Since some of the matrix elements of P could be zero, we cannot invert the equation to give D as a function of G , so we leave the relation in this form. We also point out a corollary to this theorem: all compatible purifications of the test states $\{\rho_k\}$ can be prepared by applying a CPTP map to a set of purifications which are orthogonal. Therefore, orthogonal purifications can be seen as generators for the rest of the set of purifications. Of course, we are interested in the other end of this generation, i.e., the limiting sets of purifications.

Given some ensemble of test states, it may be quite difficult to determine the best purifications analytically, especially for arbitrary test states. Alternatively, we can attempt to find limiting purifications by maximizing some objective function f , defined on ensembles of pure states (or on the corresponding Gram matrix), which preserves the order structure induced by CPTP maps. In other words, if there exists a CPTP map Ω taking the pure states $\{|\gamma_k\rangle\}_{k=0}^{M-1}$ to the pure states $\{|\delta_k\rangle\}_{k=0}^{M-1}$, the desired function must satisfy

$$f(\{|\gamma_k\rangle\}) \leq f(\{|\delta_k\rangle\}). \quad (18)$$

When this property holds, the purifications which are limiting in the sense of CPTP maps will maximize the objective function f . Before discussing candidates for the

objective function, we point out one caveat. Namely, the order structure imposed on the purifications by CPTP maps is not a total order. Accordingly, purifications which are not linked by a CPTP map are not comparable. Nevertheless, we can design quantum benchmarking schemes with any feasible set of purifications, and this heuristic provides a way to obtain strong candidates.

A good candidate for the objective function is the *Gram matrix purity* \mathcal{P} (recall from Eq. (8) that ρ_A is essentially the Gram matrix of the chosen purifications):

$$\begin{aligned} \mathcal{P} &= \text{Tr}(\rho_A^2) = \sum_{k=0}^{M-1} \sum_{l=0}^{M-1} |\langle\rho_A|_{kl}|^2 \\ &= \frac{1}{M^2} \sum_{k=0}^{M-1} \sum_{l=0}^{M-1} |\langle\Gamma_k|\Gamma_l\rangle|^2. \end{aligned} \quad (19)$$

From the above theorem, when there is a CPTP map taking $\{|\Gamma_k\rangle\} \rightarrow \{|\Delta_k\rangle\}$, we must have

$$\langle\Gamma_k|\Gamma_l\rangle = P_{kl} \langle\Delta_k|\Delta_l\rangle, \quad (20)$$

with $|P_{kl}| \leq 1$. Therefore the Gram matrix purity is monotonic with respect to CPTP maps, as required.

The Gram matrix purity also has links to the distinguishability of the test states. For example, when working with only two test states ρ_0 and ρ_1 , the maximal value of \mathcal{P} is

$$\max \mathcal{P} = \frac{1}{4} \left(2 + 2 \max_{|\Gamma_0\rangle, |\Gamma_1\rangle} |\langle\Gamma_0|\Gamma_1\rangle|^2 \right) \quad (21)$$

$$= \frac{1}{2} (1 + F(\rho_0, \rho_1)). \quad (22)$$

Aside from a fixed affine transformation, the Gram matrix purity is the fidelity between the test states. For $M > 2$, the Gram matrix purity defines a kind of averaged multi-state analog of the fidelity. Finally, consider the state

$$\rho_{A'A''} = \frac{1}{M} \sum_{k=0}^{M-1} |\Gamma_k\rangle\langle\Gamma_k|_{A'A''}. \quad (23)$$

Since a device has no information about which test state was prepared, this is the effective state input to the device in the purification picture. But since the virtual entangled state in Eq. (7) is pure, the spectra of the reduced states are equal, i.e., $\text{spec}(\rho_A) = \text{spec}(\rho_{A'A''})$. Therefore, when ρ_A is of high purity, then so is the average test state $\rho_{A'A''}$. Intuitively, when the average state $\rho_{A'A''}$ is close to a pure state, its constituent test states $\{|\Gamma_k\rangle\langle\Gamma_k|\}$ will be difficult to distinguish.

One drawback of the Gram matrix purity is that it will be difficult to compute the maximum for $M > 2$, where we do not currently have an analytic formula like Eq. (6). Alternatively, since the objective function in Eq. (19) is convex and the set of compatible Gram matrices is convex (see Appendix A), we could maximize this function numerically using the methods of convex optimization.

Although this presents one path towards our goal, we will not pursue it here.

Instead, the Gram matrix purity helps us motivate a slightly different objective function which is easier to optimize numerically. To write this alternate function, we abbreviate the overlaps by

$$Z_{kl} := \langle \Gamma_k | \Gamma_l \rangle \quad (24)$$

and decompose them into real and imaginary parts:

$$Z_{kl} = X_{kl} + iY_{kl}. \quad (25)$$

The alternate objective function is given by

$$h := \sum_{k=l+1}^{M-1} \sum_{l=0}^{M-1} (X_{kl} + Y_{kl}). \quad (26)$$

Aside from a prefactor and duplicated terms, the main difference between h and the Gram matrix purity \mathcal{P} is that the squared modulus of the overlaps is replaced by a sum of the real and imaginary parts. The advantage of this objective function is that it is linear in the parameters X_{kl} and Y_{kl} , allowing us to numerically optimize it using a semidefinite program, which can be done efficiently. In cases where the imaginary parts Y_{kl} vanish, then $X_{kl} + Y_{kl}$ is a lower bound to the modulus $|Z_{kl}|$. As well, when the objective function h is large, the Gram matrix purity will also be large, meaning we are close to a limiting Gram matrix. The main drawback of this objective function is that it is not always monotonic. Nevertheless, we remind the reader that *any* compatible Gram matrix, including one found by an optimization process over h , is valid for benchmarking purposes. Indeed, we will see in Sec. III that, despite being non-monotonic, this function leads to a Gram matrix with near-optimal purity.

Before moving on, we pause to summarize the main results of this section. Given some arbitrary ensemble of test states $\{\rho_k\}_{k=0}^{M-1}$, we consider a virtual entangled state as in Eq. (7), where the states $\{|\Gamma_k\rangle_{A'A''}\}_{k=0}^{M-1}$ are purifications of the test states. Although the test states are used in practice, we benchmark a device by assuming that the device has access to the purifications. This framework provides more power to an adversarial device, but there is also some flexibility in the choice of purifications, which can be used to restrict the adversarial advantage. We showed that purifications which are extremal in the sense of CPTP maps are better for benchmarking than all other comparable choices, so we should aim to build benchmarks using such purifications. We suggest finding good candidate purifications by optimizing some appropriate function which is monotonic with respect to CPTP maps. We propose the Gram matrix purity \mathcal{P} as a suitable candidate for this objective function, although it may be difficult to compute. We also propose a numerically simpler, though non-monotonic, objective function which may be used in place of the Gram matrix purity. After the purifications have been chosen, the benchmarking proceeds as in the pure state case (see Sec. II A), requiring only the associated Gram matrix.

D. Benchmarking with phase-symmetric ensembles

One useful application for the above results is in testing devices which are phase covariant. A device (represented by Λ) is phase covariant when it commutes with unitary rotations of phase space, i.e.,

$$\Lambda[U_\phi \sigma U_\phi^\dagger] = U_\phi \Lambda[\sigma] U_\phi^\dagger \quad \forall \sigma. \quad (27)$$

The rotation unitary is given by $U_\phi = \exp(-i\phi\hat{n})$, with \hat{n} the standard number operator, so $U_\phi^\dagger = U_{-\phi}$. We note that any channel can be made phase covariant by phase-randomization,

$$\Lambda_C[\cdot] = \frac{1}{2\pi} \int_0^{2\pi} U_\phi \Lambda[U_{-\phi}(\cdot) U_\phi^\dagger] U_\phi^\dagger d\phi. \quad (28)$$

One way to accomplish this phase randomization is to use a drifting optical phase [19], a situation which is common in many continuous-variable setups. If the phase-randomized version of a channel passes a quantum benchmark, then the channel itself must be in the quantum domain as well. On the other hand, since Λ_C involves a concatenation of channels, a phase-randomized channel may perform weaker against our benchmarks than the original channel.

Phase-covariant channels offer a number of advantages. On the experimental side, they can be benchmarked using only one physical test state. The effects of a phase-covariant channel on many other test states can be inferred by symmetry. On the theoretical side, phase covariance can lead to great numerical simplifications. If the test states are unrelated, the number of free parameters scales quadratically with the number of states M . When phase symmetry conditions are imposed, we will show that the number of free parameters can be made to scale only linearly with M . This gives us more computational room to push up the number of states M in the test ensemble, leading to stronger benchmarks.

To benchmark a phase-covariant channel, we consider test states from the rotationally-symmetric ensemble

$$\{\rho_k | \rho_k = U_\theta^k \rho_0 U_\theta^{\dagger k}\}_{k=0}^{M-1}, \quad (29)$$

where $\theta = \frac{2\pi}{M}$ (the angle θ will always be defined this way). For phase-covariant devices, we have

$$\Lambda[\rho_k] = U_\theta^k \Lambda[\rho_0] U_\theta^{\dagger k}, \quad (30)$$

so we can infer the channel's effect on ρ_k by suitable rotations of its action on one real test state ρ_0 . In this way we can generate multi-state benchmark data efficiently from any seed state. We will refer to the situation where both the test states are phase symmetric and the tested device is phase covariant as *phase-symmetric benchmarking*.

We will now present two standard form results relevant to phase-symmetric benchmarking. Given a particular device (mapping from system $A'A''$ to B), the output state ρ_{AB}^{out} is defined by

$$\rho_{AB}^{\text{out}} := [\text{id}_A \otimes \Lambda] |\Psi^{\text{ent}}\rangle\langle\Psi^{\text{ent}}|_{AA'A''}, \quad (31)$$

where $|\Psi^{\text{ent}}\rangle_{AA'A''}$ is the effective entangled state in Eq. (7). We must show that this reduced state is entangled in order to certify the given device. Without loss of generality, we can decompose this state as

$$\rho_{AB}^{\text{out}} = \frac{1}{M} \sum_{k=0}^{M-1} \sum_{l=0}^{M-1} |k\rangle\langle l|_A \otimes \rho_{kl}^{\text{out}}, \quad (32)$$

where ρ_{kl}^{out} are square matrices on the B subsystem (the diagonal blocks $\rho_{kk}^{\text{out}} = \rho_k^{\text{out}}$ are the output states). In a phase-symmetric benchmarking situation, the following relation can be imposed:

$$U_\theta \rho_{kl} U_\theta^\dagger = \rho_{k+1, l+1} \pmod{M} \quad \forall k, l. \quad (33)$$

States with this symmetry can be brought into a simple standard form:

Theorem 2 (Standard form) *Let*

$$\tau_{AB} = \frac{1}{M} \sum_{k=0}^{M-1} \sum_{l=0}^{M-1} |k\rangle\langle l|_A \otimes \tau_{kl}, \quad (34)$$

be an arbitrary bipartite matrix. Let $\theta = \frac{2\pi}{M}$ and let $\omega_M = \exp(i\theta)$ denote the primitive M th root of unity. Assume that the following symmetry relation holds:

$$U_\theta \tau_{kl} U_\theta^\dagger = \tau_{k+1, l+1} \pmod{M} \quad \forall k, l. \quad (35)$$

Then τ_{AB} is unitarily equivalent to a block diagonal matrix

$$\mathcal{D}(\tau_{AB}) = \bigoplus_{k=0}^{M-1} E_k \quad (36)$$

where

$$E_k = \frac{1}{M} \sum_{l=0}^{M-1} \omega_M^{k \cdot l} \tau_{kl} U_\theta^l. \quad (37)$$

Moreover,

$$\sum_{k=0}^{M-1} E_k = \tau_{00}, \quad (38)$$

and τ_{AB} is positive semidefinite if and only if all of the E_k are positive semidefinite.

Proof. See Appendix B.

In the next section, we will quantify the entanglement of the state ρ_{AB}^{out} by computing lower bounds on the negativity [35–38], an entanglement measure defined by

$$\mathcal{N}(\tau_{AB}) = \frac{\|\tau_{AB}^{T_A}\|_1 - \text{Tr}(\tau_{AB})}{2}, \quad (39)$$

where T_A denotes partial transposition and $\|\cdot\|_1$ is the trace norm. For phase-symmetric benchmarking, we can greatly simplify this calculation.

Theorem 3 (Trace norm in standard form) *Let τ_{AB} be as in Theorem 2. Then the trace norm of the partially transposed state $\tau_{AB}^{T_A}$ reduces to the form*

$$\|\tau_{AB}^{T_A}\|_1 = \sum_{k=0}^{M-1} \|\tilde{E}_k\|_1, \quad (40)$$

where the $\{\tilde{E}_k\}_{k=0}^{M-1}$ are formed by rearranging the matrix elements of $\{E_k\}_{k=0}^{M-1}$ from the standard form of τ_{AB} . Specifically, the matrix elements in the Fock basis are determined via

$$[\tilde{E}_k]_{jl} = [E_{j+l-k}]_{jl} \pmod{M}. \quad (41)$$

Proof. See Appendix C.

These two standard form results allow us reduce the numerical complexity of phase-symmetric benchmarking. Although the constraints remain unchanged (the Gram matrix ρ_A and measurements on the seed state ρ_0), the benchmarking state is more compactly encoded by using the M square matrices E_k instead of the $\frac{M(M+1)}{2}$ independent blocks τ_{kl} .

III. DEMONSTRATION WITH REAL MEMORY DATA

We now demonstrate the above theoretical results using real data generated by a continuous-variable memory. This memory is based on a three-level lambda gradient echo scheme involving hyperfine spin states of warm rubidium atoms. Its fundamental operation has been outlined in detail elsewhere [25]. The data used in the present paper is based on the results reported in [24]. This memory is not expected to have any sensitivity to phase. Indeed, the equations governing the memory operation are phase-independent [25]. As well, there is no experimental indication of phase sensitivity in the memory, i.e., the observed loss and excess noise are uniform with respect to the angle in phase space. Furthermore, there is no cross-talk between consecutive runs of the experiment. A data set contains measurements from 100,000 pulses stored in, and then recalled from, the memory. Each pulse was separated in time by 0.1 ms which, given the decoherence rate of the atoms in the hot gas cell, means that each pulse was stored in a fresh ensemble of atoms.

The experimental phase reference was allowed to drift freely between runs. In principle, this drift could be used to phase-randomize the device following the approach of [19], rendering the channel phase covariant. For the experimental data used in the present analysis, the observed drift was not fast enough to ensure the uniformly random distribution of phase angles required in Eq. (28). In future experiments, uniformity of the phase drift could be imposed by modifying the repetition rate of the experiment (see Sec. III A for more specific details).

However, given the very strong evidence that the memory is phase-insensitive and that consecutive runs are uncorrelated, it is reasonable to expect that the memory operation is intrinsically phase-covariant. Our goal here is to demonstrate the strength of our benchmarking approach under a variety of scenarios, by using data from a real memory. We therefore assume that running the experiment with a completely uniform phase drift would lead to the same data as obtained at the current repetition rate. In other words, the obtained experimental data is assumed to come from a phase-covariant memory. The phase-covariance assumption, which is independent from the benchmarking theory, allows us to easily generate a number of different test ensembles using data from a single seed state, i.e., we have many non-orthogonal test states $\{\rho_k | \rho_k = U_\theta^k \rho_0 U_\theta^{\dagger k}\}_{k=0}^{M-1}$. To fully certify the memory with no assumptions (i.e., where we treat the memory as a black box) would require a more uniform phase drift than we obtained. Nevertheless, the current scenario allows for a useful demonstration of our benchmarking tools.

A. Experimental data acquisition

During an experimental run, light is generated from a continuous-wave master laser and split into a coupling field (for activating the memory), a strong continuous-wave local oscillator, a weak signal pulse, and a memory-reference pulse. The memory-reference pulse is detuned from the active frequencies of the memory (while maintaining a well-defined phase relation with the signal pulse), so that it passes through the memory without absorption. The signal pulse is sent to the memory shortly after the reference pulse such that the phase drift between the two pulses can be neglected. Thus, we can obtain phase information for the input signal by determining the phase of the memory-reference pulse.

Both the output signal and memory-reference pulses are interfered with the local oscillator (which has not passed through the memory) in a homodyne measurement scheme. Data was collected using a 12-bit resolution data acquisition system. The homodyne measurement angle is varied between runs by allowing the signal and local oscillator to freely drift. This phase angle is identified by fitting a sine wave to the memory-reference pulse. A quadrature value was assigned to each signal pulse after interference with the local oscillator by integrating the amplitude of the pulse over its duration. Note that any inherent frequency shift due to the memory was cancelled coherently by adjusting the external magnetic field applied to the memory before data collection. This process generates quadrature measurement data for the output state ρ_0^{out} . Similar data is obtained for the input state ρ_0 by measuring it after it passes through an inactive memory [40].

Over repeated runs, many data points are collected to form a raw data set covering many phase angles. To en-

Operator	First moment $\langle \cdot \rangle$	Second moment $\langle \cdot \rangle^2$
\hat{x}	0.01 ± 0.03	0.57 ± 0.04
\hat{p}	-0.95 ± 0.03	1.41 ± 0.09

TABLE I: Experimentally-determined first and second moments for the conjugate quadratures \hat{x} and \hat{p} . The vacuum state would have variances $\text{Var}(\hat{x}) = \text{Var}(\hat{p}) = \frac{1}{2}$ in these units.

sure complete randomisation of the input pulse, the drift resulting from thermal fluctuations needs to be much faster than the repetition rate of the experiment. In our experimental setup, the pulse's thermal drift occurred at a rate on the order of Hz, while the experimental data was taken at a kHz rate. Running the experiment at a slower repetition rate would allow the phase reference enough time to fully randomize, making the phase-randomization procedure of [19] possible and guaranteeing phase-covariance. Of course, this would also affect the time needed to acquire the experimental data.

Tomographic reconstruction was performed using an iterative maximum-likelihood algorithm [41] using data from 100,000 pulses, giving density matrices for both the input and output states in the Fock basis. A constant memory-induced phase offset [42] between the input and output signals was observed, and cancelled digitally during the tomography step. The tomographically-reconstructed density matrices were numerically truncated after the first 30 Fock states ($|0\rangle, \dots, |29\rangle$). This cutoff is supported by the fact that both the input state and output state are essentially confined to the first 10 Fock levels, for which the cutoff error in either state is $\approx 10^{-5}$. From the tomography, the input state was found to have mean photon number $\langle \hat{n}_{\text{in}} \rangle = 0.67$ [24]. This value is consistent with the value obtained using direct quadrature measurement [43]. We do not explicitly categorize this state, but it is qualitatively a 'coherent state with added noise'. This extra noise is primarily due to amplitude fluctuations and changes in mode-matching occurring during the testing process. The tomographically-reconstructed output state had a similar form, with mean photon number $\langle \hat{n}_{\text{out}} \rangle = 0.57$.

As stated in Sec. II A, output state tomography is not required in quantum benchmarking; measurement of two conjugate quadratures may be sufficient. To compare the two approaches, we also consider benchmarks using measurements from only \hat{x} and \hat{p} . To get the required expectation values, we collected the original quadrature/phase data into bins containing 500 data points and restricted our attention to two bins corresponding to phase angles of 0 and 90 degrees. Taking the mean and standard deviation of the data within these bins, we get estimates of $\langle \hat{x} \rangle$, $\langle \hat{p} \rangle$, $\text{Var}(\hat{x})$, and $\text{Var}(\hat{p})$, where $\text{Var}(\hat{z}) = \langle \hat{z}^2 \rangle - \langle \hat{z} \rangle^2$ for an operator $\hat{z} \in \{\hat{x}, \hat{p}\}$. Error bars, based on the finite sample size of the bins, are calculated using standard error propagation techniques. The final quadrature moment values are listed in Table I.

B. Finding the Gram matrix

The test ensemble is generated by rotations of the seed state ρ_0 , as in Eq. (29), forming a ring in phase space. Our theoretical description of the seed state comes from the tomographic reconstruction with the finite cutoff in Fock space. We make no further assumptions about the seed state other than that the tomographic description is accurate. Purifications, and the associated Gram matrix, will be based on this numerical description. Due to the mixed nature of this state, previous entanglement-based benchmarking schemes would be limited to only two test states. We will see later that two test states are not sufficient in this case to reliably (i.e., within experimental error) give non-zero output entanglement, but adding more test states enables a successful benchmarking.

In order to find candidate Gram matrices for the purifications, we convert the optimization to a semidefinite program. To this end, we consider the bipartite matrix

$$\begin{aligned} \rho_{AA'}^{\text{in}} &= \text{Tr}_{A''} |\Psi^{\text{ent}}\rangle\langle\Psi^{\text{ent}}|_{AA'A''} \\ &= \frac{1}{M} \sum_{k=0}^{M-1} \sum_{l=0}^{M-1} |k\rangle\langle l|_A \otimes \rho_{kl}^{\text{in}}. \end{aligned} \quad (42)$$

The diagonal blocks of $\rho_{AA'}^{\text{in}}$ are the test states, i.e., $\rho_{kk}^{\text{in}} = \rho_k$, and the off-diagonal blocks ρ_{kl}^{in} consist of free parameters. The off-diagonal blocks are linked to the purifications through the relation

$$\text{Tr}(\rho_{kl}^{\text{in}}) = M \langle k | \rho_A | l \rangle = \langle \Gamma_l | \Gamma_k \rangle. \quad (43)$$

We have traced out the purifying system A'' since no measurements are performed on that system, but we have kept subsystem A' in order to later ascribe some quantity of entanglement to the input state.

As stated in Sec. II C, instead of using the Gram matrix purity \mathcal{P} , we optimized the slightly different and numerically more simple objective function h from Eq. (26). Although it might be more elegant to use the Gram matrix purity \mathcal{P} , nothing in the benchmarking procedure depends on that function. In fact, the Gram matrix found by optimizing h over the given experimental data works quite well for our purposes. To see this, we can consider simple lower and upper bounds on the maximum value of \mathcal{P} compatible with the given constraints.

For one, the purity of the Gram matrix that maximizes h (denoted $\arg \max h$) is less than the maximum possible Gram matrix purity over all purifications, i.e.,

$$\mathcal{P}|_{\arg \max h} \leq \max \mathcal{P}. \quad (44)$$

On the other hand, we can easily find an upper bound on \mathcal{P} by considering the pairwise fidelities:

$$\max \mathcal{P} \leq \frac{1}{M^2} \sum_{k=0}^{M-1} \sum_{l=0}^{M-1} F(\rho_k, \rho_l). \quad (45)$$

In Fig. 1, we plot the values of these lower and upper bounds for different numbers of rotationally symmetric

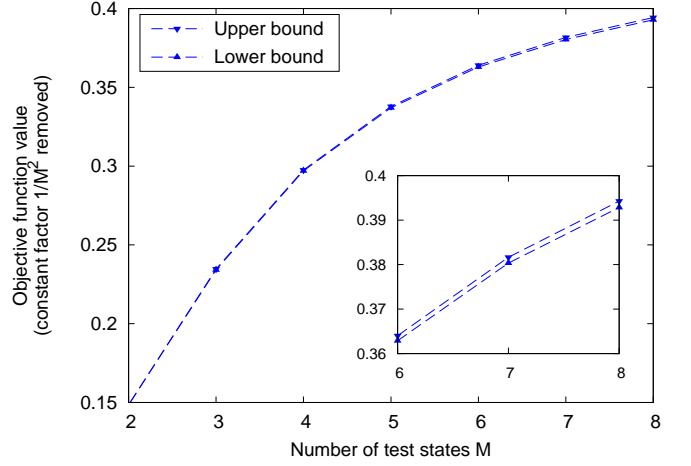


FIG. 1: Upper and lower bounds for the maximum purity \mathcal{P} of experimentally-compatible Gram matrices, corresponding to rotationally symmetric test ensembles of different cardinality. We have removed the factor $\frac{1}{M^2}$, which is common to both the upper and lower bounds, and independent of the purifications. The difference between the two bounds is on the order of 10^{-3} or less (inset), meaning that the obtained Gram matrix has purity which is near-optimal (represented by the lower curve). The estimated numerical precision of the optimization is $\approx 10^{-3}$.

test states (omitting the constant factors $\frac{1}{M^2}$). The computed bounds are very close to each other, differing only in the third decimal place, which is the same order as the estimated numerical precision of our optimization. We conclude that using the modified objective function in Eq. (26) is suitable for the situation we are considering, and that the obtained Gram matrix purity is close to what would be obtained by maximizing \mathcal{P} itself.

C. Computing the entanglement

Having used the heuristic function h to find a feasible $\rho_{AA'}^{\text{in}}$ which corresponds to a near-optimal Gram matrix, we now consider the entanglement of the corresponding output state ρ_{AB}^{out} . We use the negativity as our entanglement measure, which can be computed as a semidefinite program, namely

$$\mathcal{N}(\tau_{AB}) = \min_{\tau_- \in \Upsilon} \text{Tr}(\tau_-), \quad (46)$$

where the constraint set Υ is defined by

$$\Upsilon := \{\tau_- | \tau_- \geq 0 \text{ and } \tau_{AB}^T + \tau_- \geq 0\}. \quad (47)$$

For optimizations where τ_{AB} is not fully known (as is the situation here), constraints from experimental observations are also included in this set. For states written in standard form, the negativity can be computed on the level of the individual matrices E_k .

Next, we used the entanglement quantification tools from [21] to compute the lowest value of the negativity that could be compatible with the given data. In

this approach, one rigorously finds lower bounds on the negativity of the output state ρ_{AB}^{out} by truncating the B subsystem of the density matrix at some finite Fock level N , which is large compared to the observed mean photon number \bar{n} . For this test, we imposed the cutoff at Fock level $N = 15$, making the truncated matrices 16-dimensional.

The quantification procedure was applied to four measurement scenarios:

- (i) **Tomography**: the output density matrix is fully known numerically (up to the truncation level N);
- (ii) **Quadratures from tomography**: only measurements on conjugate quadratures \hat{x} and \hat{p} for the output state are used, and these values are obtained from the tomographically-reconstructed density matrix;
- (iii) **Quadratures from data**: same as (ii), but the quadrature values are obtained directly from the homodyne data;
- (iv) **Quadratures with error bars**: the same quadrature data is used as in (iii), but estimates of data error bars are included in the computation ($\sigma - 3\sigma$ levels).

In cases (ii)-(iv), the choice of N affects the strength of the optimization procedure itself [21], not just the density matrix. Truncating at a higher level would lead to better bounds on the entanglement. In all cases, we use the standard form results of Theorems 2 and 3. Finally, although [21] does not explicitly give a procedure for including error bars in the computation, it is straightforward to relax the framework and include them. We performed the optimization in Matlab, using the frontend YALMIP [44] and the solver SDPT3 [45]. The numerical precision of the optimization is estimated to be $\approx 10^{-3}$. The results of these computations for different sized rotationally-symmetric ensembles is shown in Figs. 2 and 3.

There are a number of things to point out about the results in Figs. 2 and 3. Primarily, we see that our benchmarking tools were successful in finding non-zero output entanglement in this phase-symmetric situation. Not only is the output state ρ_{AB}^{out} entangled for all M when we use the tomographically reconstructed density matrix ρ_0^{out} , but we can also see non-zero entanglement using the restricted set of measurements, including error bars. Furthermore, there is an evident advantage in using more than two test states, since it leads to higher entanglement in all cases. Indeed, it is not until $M > 2$ that the 3σ level conclusively leads to non-zero entanglement in the output state.

Another interesting result is that scenarios (i) and (ii) give very similar results for the entanglement when $M \geq 3$. This is likely due to the fact that the output state has low levels of excess noise. The quadratures would already reveal that such a state is close to a minimum

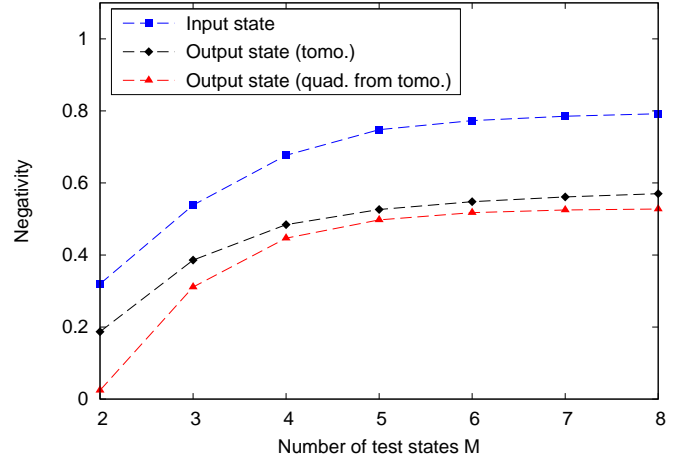


FIG. 2: Benchmarking results based on rotationally-symmetric test ensembles using tomographically-reconstructed density matrices. The top curve is the negativity of the input state $\rho_{AA'}^{\text{in}}$ found by optimizing the heuristic function h . The other curves are lower bounds to the negativity of ρ_{AB}^{out} based on (in descending order): (i) tomographic reconstruction and (ii) quadrature values obtained from the tomographic reconstruction. A benchmarking procedure is successful when the output state has negativity larger than zero.

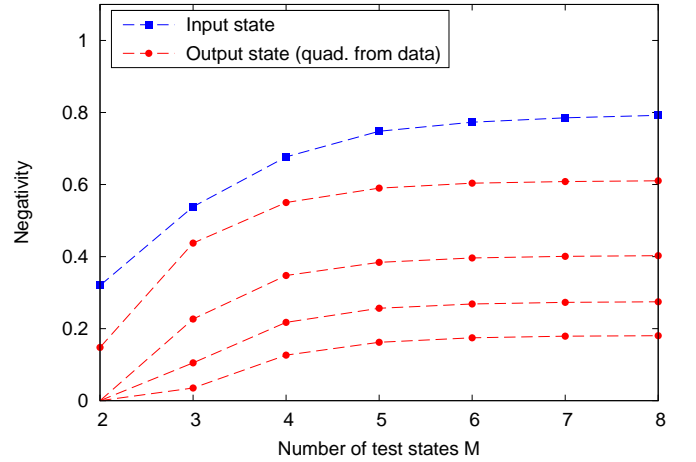


FIG. 3: Benchmarking results based on rotationally-symmetric test ensembles using direct quadrature measurement data. The top curve is the same as Fig. 2. The other curves are lower bounds to the negativity of ρ_{AB}^{out} based on (in descending order): (iii) quadrature values obtained directly from measurement data and (iv) quadrature data with error bars included in the optimization (1σ , 2σ , and 3σ levels). For more than 3 test states, there is non-zero entanglement remaining even when including error estimates.

uncertainty state. Additional measurement information therefore does not contribute significantly to our knowledge of the state. For other types of states, quadrature measurements and tomography should not be expected to yield similar results (though there may be other choices

of measurement operators which work well). Note that we do not compare situations (i) and (iii) because of the extra phase shift included in the tomographic reconstruction outlined in Sec. III A.

We also point out the advantage offered by phase-symmetric benchmarking and the standard form. Previously, entanglement quantification results were demonstrated for test ensembles consisting of only two or three states [20, 21]. Although the methods of [21] apply to any number of (pure) test states, the computational resources required for more than three test states were prohibitive. Here, using the standard form, we have no problem pushing up to much higher numbers of states; Figs. 1-3 contain results for up to 8 test states. In fact, with a desktop PC, we were able to calculate benchmarks for up to 10 states, but these results are not included in the figures because they do not significantly change after $M = 8$. Finally, we note that all the results for the output state entanglement are lower bounds. If we were to use a real entangled state instead of a virtual one, we would have access to more information, and the output entanglement would be higher. Even still, for benchmarking schemes based on a virtual entangled state, the entanglement quantification procedure yields useful and illuminating results.

IV. CONCLUSION

We have extended the methodology for entanglement-based quantum benchmarking to arbitrary finite ensembles of test states. This extension considers purifications of the test states, and we have outlined how to find strong choices for these purifications, leading to the best chance of certifying a device in the quantum domain. We also gave equations for reducing the test states to a standard form when certain phase symmetry conditions hold, allowing us to generate benchmarks from any single seed state. These theoretical tools were demonstrated using data from a real-world quantum memory and to quantitatively explore different benchmarking scenarios. Although we mainly considered test states which were of a continuous-variable nature, all of our results, except the standard form, apply to discrete states as well. Indeed, the same framework can be used to calculate fidelity-based benchmarks, which may be better suited to low-dimensional states [46]. Since our benchmarking scheme works for arbitrary test states, it incorporates previous entanglement-based benchmarking tools [15–21] into a unified framework. Together, these tools allow us to perform efficient benchmarking tests on quantum devices using realistic experimental resources.

Acknowledgments

N.K. and N.L. acknowledge support from an NSERC Discovery Grant, Quantum Works, and Ontario Cen-

tres of Excellence. N.K. acknowledges additional support from the Ontario Graduate Scholarship Program. The ANU group acknowledges support from the Australian Research Council Centre of Excellence for Quantum Computation and Communication Technology (Project number CE110001027).

Appendix A: Convexity proofs

In this appendix, we prove the following two statements about convexity: i) the objective function in Eq. (19) is a convex function, and ii) the set of Gram matrices which are consistent with purifications of the test states is a convex set. First, for positive semidefinite operators, the purity is equivalent to the squared Hilbert-Schmidt norm. By definition, all norms are convex, and taking the square preserves this convexity. Hence, our objective function is convex.

To prove the second statement, let $\{|\Gamma_k^0\rangle_{A'A''}\}_{k=0}^{M-1}$ and $\{|\Gamma_k^1\rangle_{A'A''}\}_{k=0}^{M-1}$ be two sets of purifications of the test states $\{\rho_k\}_{k=0}^{M-1}$ (without loss of generality, we can consider the purifying system to be the same), with Gram matrices G_0 and G_1 , respectively. Fix some $p \in [0, 1]$ and take the convex combination of Gram matrices $G = pG_0 + (1-p)G_1$. We need to show that there is some compatible set of purifications leading to the Gram matrix G .

To do this, we define the following states:

$$|\chi_k\rangle_{A'A''A'''} := \sqrt{p} |\Gamma_k^0\rangle_{A'A''} |0\rangle_{A'''} + \sqrt{1-p} |\Gamma_k^1\rangle_{A'A''} |1\rangle_{A'''}, \quad (\text{A1})$$

where $|0\rangle_{A'''}$ and $|1\rangle_{A'''}$ are orthonormal states on some additional purifying system A''' . Tracing out all systems except A' , we find

$$\begin{aligned} \text{Tr}_{A''A'''} |\chi_k\rangle\langle\chi_k|_{A'A''A'''} &= p \text{Tr}_{A''} |\Gamma_k^0\rangle\langle\Gamma_k^0|_{A'A''} \\ &\quad + (1-p) \text{Tr}_{A''} |\Gamma_k^1\rangle\langle\Gamma_k^1|_{A'A''} \\ &= \rho_k. \end{aligned} \quad (\text{A2})$$

Thus, the $|\chi_k\rangle_{A'A''A'''}$ are purifications of the ρ_k . The elements of the corresponding Gram matrix are

$$\begin{aligned} \langle\chi_k|\chi_l\rangle &= p \langle\Gamma_k^0|\Gamma_l^0\rangle + (1-p) \langle\Gamma_k^1|\Gamma_l^1\rangle \\ &= p[G_0]_{kl} + (1-p)[G_1]_{kl}, \end{aligned} \quad (\text{A3})$$

which are exactly the elements of the convex combination G . Therefore, the set of Gram matrices which come from purifications of the test states is a convex set.

Appendix B: Proof of standard form

In this appendix, we give the proof of the standard form in Theorem 2. If Eq. (35) holds, then τ_{AB} can be

transformed by the unitary matrix

$$R = \bigoplus_{k=0}^{M-1} U_{\theta}^k \quad (\text{B1})$$

to the form

$$\begin{aligned} \mathcal{C}(\tau_{AB}) &= R^{\dagger} \tau_{AB} R \\ &= \frac{1}{M} \begin{bmatrix} \tau_{00} & W_{01} & W_{02} & \cdots & W_{0,M-1} \\ W_{0,M-1} & \tau_{00} & W_{01} & \cdots & W_{0,M-2} \\ W_{0,M-2} & W_{0,M-1} & \tau_{00} & \cdots & W_{0,M-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ W_{01} & W_{02} & W_{03} & \cdots & \tau_{00} \end{bmatrix} \end{aligned} \quad (\text{B2})$$

with $W_{ij} := \tau_{ij} U_{\theta}^j$. The matrix $\mathcal{C}(\tau_{AB})$ has a *block circulant* structure, meaning that each row of blocks is the same as the previous row, but shifted by one to the right. Now, let $\omega_M = \exp(i\theta)$ be the primitive M th root of unity and let

$$[F_M]_{ij} = \frac{1}{\sqrt{M}} \omega_M^{i \cdot j} \quad (\text{B3})$$

be the (unitary) discrete Fourier transform matrix. Using a standard theorem on block circulant matrices [47], $\mathcal{C}(\tau_{AB})$ can be block diagonalized by the matrix $F_M \otimes \mathbb{1}_B$. Explicitly,

$$\begin{aligned} \mathcal{D}(\tau_{AB}) &= (F_M^{\dagger} \otimes \mathbb{1}_B) \mathcal{C}(\tau_{AB}) (F_M \otimes \mathbb{1}_B) \\ &= \bigoplus_{k=0}^{M-1} E_k, \end{aligned} \quad (\text{B4})$$

with

$$E_k = \frac{1}{M} \sum_{l=0}^{M-1} \omega_M^{k \cdot l} W_{kl} \quad (\text{B5})$$

Since the partial trace is unaffected by local unitaries on the same subsystem, we have

$$\begin{aligned} \sum_{k=0}^{M-1} E_k &= \text{Tr}_A \left(\sum_{k=0}^{M-1} |k\rangle\langle k|_A \otimes E_k \right) \\ &= \text{Tr}_A \mathcal{D}(\tau_{AB}) \\ &= \text{Tr}_A \mathcal{C}(\tau_{AB}). \end{aligned} \quad (\text{B6})$$

Comparing this with Eq. (B2), we conclude

$$\sum_{k=0}^{M-1} E_k = \tau_{00}, \quad (\text{B7})$$

which proves Eq. (38). Finally, the positive semidefinite condition follows directly from the unitary equivalence of τ_{AB} and $\mathcal{D}(\tau_{AB})$. \square

Appendix C: Proof of trace norm in standard form

In this appendix, we prove Theorem 3, which gives a formula for the negativity involving the standard form. If τ_{AB} satisfies the symmetry condition in Eq. (35), then so will the partial transpose τ_{AB}^{TA} . Therefore, τ_{AB}^{TA} is unitarily equivalent to some block diagonal matrix $\mathcal{B}(\tau_{AB}^{TA}) = \bigoplus_{k=0}^{M-1} \tilde{E}_k$. The trace norm is a unitarily invariant norm, so we must have

$$\|\tau_{AB}^{TA}\|_1 = \left\| \bigoplus_{k=0}^{M-1} \tilde{E}_k \right\|_1 = \sum_{k=0}^{M-1} \|\tilde{E}_k\|_1, \quad (\text{C1})$$

which proves Eq. (40).

In order to determine the matrices \tilde{E}_k in Eq. (41), we first find an explicit expression relating the standard form matrices E_k and the matrix τ_{AB} . Define the matrix elements of a bipartite matrix H by

$$[H]_{ij,kl} := \langle i|_A \otimes \langle j|_B H |k\rangle_A \otimes |l\rangle_B. \quad (\text{C2})$$

For subsystem B , we work in the Fock basis, where the rotation operator U_{θ} is diagonal, with elements

$$[U_{\theta}]_{jl} = \omega_M^{-j} \delta_{jl}. \quad (\text{C3})$$

The unitary matrix R in Eq. (B1), formed by taking powers of U_{θ} , is also diagonal in this basis, with the following elements:

$$[R]_{ij,kl} = \omega_M^{-i \cdot j} \delta_{ik} \delta_{jl}. \quad (\text{C4})$$

Therefore, the Fock basis elements of the block circulant matrix $\mathcal{C}(\tau_{AB})$, defined in Eq. (B2), are given by

$$[\mathcal{C}(\tau_{AB})]_{ij,kl} = \omega_M^{i \cdot j - k \cdot l} [\tau_{AB}]_{ij,kl} \quad (\text{C5})$$

To get the standard form, we need to perform a Fourier transform on the block circulant matrix $\mathcal{C}(\tau_{AB})$ as in Eq. (B4). The elements of the discrete Fourier transform F_M are given in Eq. (B3). After substitution, we arrive at the matrix elements of the standard form:

$$\begin{aligned} [\mathcal{D}(\tau_{AB})]_{ij,kl} &= \frac{1}{M} \sum_{m=0}^{M-1} \sum_{n=0}^{M-1} \omega_M^{n \cdot k - i \cdot m} [\mathcal{C}(\tau_{AB})]_{mj,nl} \\ &= \frac{1}{M} \sum_{m=0}^{M-1} \sum_{n=0}^{M-1} \omega_M^{m(j-i) + n(k-l)} [\tau_{AB}]_{mj,nl}. \end{aligned} \quad (\text{C6})$$

Since $\mathcal{D}(\tau_{AB})$ is block diagonal, $\mathcal{D}(\tau_{AB}) = \bigoplus_{k=0}^{M-1} E_k$, we have

$$\begin{aligned} [E_k]_{jl} &:= [\mathcal{D}(\tau_{AB})]_{kj,kl} \\ &= \frac{1}{M} \sum_{m=0}^{M-1} \sum_{n=0}^{M-1} \omega_M^{m(j-k) + n(k-l)} [\tau_{AB}]_{mj,nl}. \end{aligned} \quad (\text{C7})$$

This is the final formula linking the elements of τ_{AB} and the matrices $\{E_k\}_{k=0}^{M-1}$. For completeness, the inverse formula is given by

$$[\tau_{AB}]_{ij,kl} = \frac{1}{M} \sum_{m=0}^{M-1} \omega_M^{m(i-k)+k \cdot l - i \cdot j} [E_m]_{jl}. \quad (\text{C8})$$

When τ_{AB}^A is used in this formula instead of τ_{AB} , we find the relation

$$[\tilde{E}_k]_{jl} := \frac{1}{M} \sum_{m=0}^{M-1} \sum_{n=0}^{M-1} \omega_M^{m(j-k)+n(k-l)} [\tau_{AB}]_{nj,ml}. \quad (\text{C9})$$

Hence, the the matrix \tilde{E} indexed by $(j+l-k)$ has elements

$$[\tilde{E}_{j+l-k}]_{jl} = \frac{1}{M} \sum_{m=0}^{M-1} \sum_{n=0}^{M-1} \omega_M^{m(k-l)+n(j-k)} [\tau_{AB}]_{nj,ml}, \quad (\text{C10})$$

which is the same as Eq. (C7), after interchanging the summation indices m and n . Therefore, $[\tilde{E}_{j+l-k}]_{jl} = [E_k]_{jl}$ (in the Fock basis).

-
- [1] C. Wittmann, J. Fürst, C. Wiechers, D. Elser, H. Häsel, N. Lütkenhaus, and G. Leuchs, *Opt. Express* **18**, 4499 (2010).
 - [2] A. I. Lvovsky, B. C. Sanders, and W. Tittel, *Nat. Photon.* **3**, 706 (2009).
 - [3] A. M. Lance, T. Symul, V. Sharma, C. Weedbrook, T. C. Ralph, and P. K. Lam, *Phys. Rev. Lett.* **95**, 180503 (2005).
 - [4] S. L. Braunstein, C. A. Fuchs, and H. J. Kimble, *J. Mod. Opt.* **47**, 267 (2000).
 - [5] S. L. Braunstein, C. A. Fuchs, H. J. Kimble, and P. van Loock, *Phys. Rev. A* **64**, 022321 (2001).
 - [6] F. Grosshans and P. Grangier, *Phys. Rev. A* **64**, 010301 (2001).
 - [7] K. Hammerer, M. M. Wolf, E. S. Polzik, and J. I. Cirac, *Phys. Rev. Lett.* **94**, 150503 (2005).
 - [8] R. Namiki, *Phys. Rev. A* **78**, 032333 (2008).
 - [9] R. Namiki, M. Koashi, and N. Imoto, *Phys. Rev. Lett.* **101**, 100502 (2008).
 - [10] G. Adesso and G. Chiribella, *Phys. Rev. Lett.* **100**, 170503 (2008).
 - [11] M. Owari, M. B. Plenio, E. S. Polzik, A. Serafini, and M. M. Wolf, *New J. Phys.* **10**, 113014 (2008).
 - [12] G. Hétet, A. Peng, M. T. Johnsson, J. J. Hope, and P. K. Lam, *Phys. Rev. A* **77**, 012323 (2008).
 - [13] J. Calsamiglia, M. Aspachs, R. Muñoz-Tapia, and E. Bagan, *Phys. Rev. A* **79**, 050301 (2009).
 - [14] M. Guță, P. Bowles, and G. Adesso, *Phys. Rev. A* **82**, 042310 (2010).
 - [15] J. Rigas, O. Gühne, and N. Lütkenhaus, *Phys. Rev. A* **73**, 012341 (2006).
 - [16] J. Rigas, Diploma thesis, University of Erlangen-Nuremberg (2006).
 - [17] H. Häsel, T. Moroder, and N. Lütkenhaus, *Phys. Rev. A* **77**, 032303 (2008).
 - [18] H. Häsel and N. Lütkenhaus, *Phys. Rev. A* **80**, 042304 (2009).
 - [19] H. Häsel and N. Lütkenhaus, *Phys. Rev. A* **81**, 060306 (2010).
 - [20] N. Killoran, H. Häsel, and N. Lütkenhaus, *Phys. Rev. A* **82**, 052331 (2010).
 - [21] N. Killoran and N. Lütkenhaus, *Phys. Rev. A* **83**, 052320 (2011).
 - [22] M. Lobino, D. Korystov, C. Kupchak, E. Figueroa, B. C. Sanders, and A. I. Lvovsky, *Science* **322**, 563 (2008).
 - [23] M. Lobino, C. Kupchak, E. Figueroa, and A. I. Lvovsky, *Phys. Rev. Lett.* **102**, 203601 (2009).
 - [24] M. Hosseini, G. Campbell, B. M. Sparkes, P. K. Lam, and B. C. Buchler, *Nat. Phys.* **7**, 794 (2011).
 - [25] M. Hosseini, B. M. Sparkes, G. T. Campbell, P. K. Lam, and B. C. Buchler, *J. Phys. B: At. Mol. Opt. Phys.* **45**, 124004 (2012).
 - [26] C. A. Fuchs and M. Sasaki, *Quant. Inf. Comp.* **3**, 377 (2003).
 - [27] M. Horodecki, P. W. Shor, and M. B. Ruskai, *Rev. Math. Phys.* **15**, 629 (2003).
 - [28] S. Lorenz, J. Rigas, M. Heid, U. L. Andersen, N. Lütkenhaus, and G. Leuchs, *Phys. Rev. A* **74**, 042326 (2006).
 - [29] A. Uhlmann, *Rep. Math. Phys.* **9**, 273 (1976).
 - [30] R. Jozsa, *J. Mod. Opt.* **41**, 2315 (1994).
 - [31] For example, when the entangled state in Eq. (7) has maximal entanglement, the purifications must be orthogonal, $\langle \Gamma_k | \Gamma_l \rangle = \delta_{kl}$. But orthogonal purifications can be perfectly distinguished and reproduced by a particular MP channel, giving the same output as a perfect quantum memory. Thus, no benchmarking protocol where Eq. (7) is maximally entangled will be successful.
 - [32] A. Uhlmann, *Wiss. Z. KMU Leipzig, Math.-Naturwiss. R.* **34**, 580 (1985).
 - [33] A. Chefles, *Phys. Lett. A* **270**, 14 (2000).
 - [34] A. Chefles, R. Jozsa, and A. Winter, *Int. J. Quant. Info.* **2**, 11 (2004).
 - [35] K. Życzkowski, P. Horodecki, A. Sanpera, and M. Lewenstein, *Phys. Rev. A* **58**, 883 (1998).
 - [36] J. Lee, M. S. Kim, Y. J. Park, and S. Lee, *J. Mod. Opt.* **47**, 2151 (2000).
 - [37] G. Vidal and R. F. Werner, *Phys. Rev. A* **65**, 032314 (2002).
 - [38] M. B. Plenio, *Phys. Rev. Lett.* **95**, 090503 (2005).
 - [39] G. Hétet, Ph.D. thesis, Australian National University (2008).
 - [40] Note that we assume the test states are not affected by an inactive memory.
 - [41] J. Řeháček, Z. Hradil, and M. Ježek, *Phys. Rev. A* **63**, 040303 (2001).
 - [42] G. Hétet, J. J. Longdell, A. L. Alexander, P. K. Lam, and M. J. Sellars, *Phys. Rev. Lett.* **100**, 023601 (2008).
 - [43] J. G. Webb, T. C. Ralph, and E. H. Huntington, *Phys. Rev. A* **73**, 033808 (2006).
 - [44] J. Löfberg, in *Proceedings of the CACSD Conference* (IEEE, Taipei, Taiwan, 2004), available from

- <http://users.isy.liu.se/johanl/yal mip/>.
- [45] K. Toh, M. Todd, and R. Tutuncu, Optimization Methods and Software **11**, 545 (1999), available from <http://www.math.nus.edu.sg/~mattohk/sdpt3.html>.
- [46] N. Killoran, Ph.D. thesis, University of Waterloo (2012).
- [47] P. J. Davis, *Circulant matrices*, 2nd. ed. (AMS Chelsea Publishing, 1994).